Information Security Tips

Ten Things you can do to Help Protect Yourself

- Passwords: Use a complex password and change it regularly. Do not use names, birthdays, or other personal details that might be easily determined.
- If you need to write down your usernames and/or passwords, be sure they are maintained in a secure place.
- Keep your computer and/or network software patches and virus protection software up to date.
- Set up a firewall to detect and prevent intrusions into your environment.
- Take advantage of all security options provided to you by your bank.
- Review your banking transactions on a daily basis and credit report on at least an annual basis.
- Store extra checks, credit cards, documents that list your Social Security number and similar items in a safe place. Shred all credit card receipts and solicitations, ATM receipts, bank account and credit card statements, canceled checks and other financial documents before you throw them away.
- Use the latest versions of Internet browsers, such as Explorer, Firefox or Google Chrome with “pop-up” blockers.
- Do not batch approve transactions; be sure to review and approve each one individually.
- Turn off your computer when not in use.

Identity Theft

Identity theft occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your reputation. Below are recommendations from the Federal Trade Commission to help combat the threat of identity theft.

1. **Deter identity thieves by safeguarding your information.**

    - **Shred financial documents** and paperwork with personal information before you discard them.

    - **Protect your Social Security number**. Don’t carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.

    - **Don’t give out personal information** on the phone, through the mail or over the Internet unless you know the entity you are dealing with. Avoid disclosing personal financial information when using public wireless connections.

- **Never click on links sent in unsolicited emails**. Instead, type in the source page of the website using a separate tab or window. Use firewalls, anti-spyware and anti-virus software to help protect your home computer. Keep such software current. If you use peer file sharing, check the settings to make sure you are not sharing other sensitive private files.

- **Don't use an obvious password**. Avoid using passwords like birth date, address, mother's maiden name, children's name or the last four digits of your Social Security number.

- **Keep your personal information in a secure place** at home, especially if you have roommates, employ outside help or are having work done in your house.

2. **Detect suspicious activity by routinely monitoring your financial accounts and billing statements.**

   - Be alert to the following signs that require immediate attention:

     - Bills do not arrive as expected
     - Unexpected credit cards or account statements
     - Denials of credit for no apparent reason
     - Calls or letters about purchases you did not make
     - Charges on your financial statements that you don't recognize

   - **Inspect your credit report.** Credit reports contain information about you, including what accounts you have and your bill paying history.

   - The law requires the major nationwide credit reporting companies Equifax, Experian and TransUnion to give you a free copy of your credit report every 12 months if you request it.

   - Visit www.AnnualCreditReport.com or call 1-877-322-8228, a service created by these three companies, to order your free annual credit report. You can also write to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, Georgia 30348-5281.

   - If you see accounts or addresses you don't recognize or information that is inaccurate, contact the credit reporting company and the information provider. To find out how to correct errors on your credit report, visit ftc.gov/idtheft.

3. **Defend against ID theft as soon as you suspect it.**

   - **Place a "Fraud Alert" on your credit reports, and review the reports carefully**. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing account. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:

     Experian: 1-888-EXPERIAN (397-3742)

     TransUnion: 1-800-680-7289

     Equifax: 1-800-525-6285

   - Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open and debts on your accounts that you can't explain.

- Contact the security or fraud departments of each company where an account was opened or charged without your authorization.
- Follow up in writing, with copies of supporting documents.
- Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
- Ask for verification that the disputed account has been dealt with and the fraudulent debts discharged.
- Keep copies of documents and records of your conversations about the theft.
- **File a police report**. File a report with law enforcement officials to help expedite the correction of your credit report and deal with creditors who may want proof of the crime.
- **Report the theft to the Federal Trade Commission**. Your report helps law enforcement officials across the country in their investigations.
- Online: ftc.gov/idtheft
- By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261
- By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

Additional Resources

FDIC Consumer News
https://www.fdic.gov/consumers/consumer/news/index.html

Federal Trade Commission (FTC)
https://www.consumer.ftc.gov/features/feature-0014-identity-theft

OnGuardOnline.Gov
https://www.consumer.ftc.gov/features/feature-0038-onguardonline

IdTheftinfo.org
http://www.idtheftinfo.org/

Office of the Comptroller of the Currency
https://occ.gov/topics/consumer-protection/fraud-resources/index-fraud-resources.html

U.S. Computer Emergency Readiness Team
https://www.us-cert.gov/

Internet Crime Complaint Center
https://www.ic3.gov/default.aspx